

CYBER LIABILITY FROM GOVERNMENT USE OF SOCIAL MEDIA

1. SOCIAL MEDIA 101?

- a. What is Social Media?
 - i. Social Media Types
 - 1. Social Networking
 - 2. Multimedia Sharing
 - 3. Blogs
- b. Employee Use of Social Networking Platforms: Deloitte 2009 Survey
 - i. 55% of employees visit social networking sites at least once a week.
 - ii. 20% of employees admit to visiting social networking sites during work hours.
 - iii. Facebook experienced a 276% rise in its 35- to 54- year-old demographic in a 6-month period.

2. GOVERNMENT USE OF SOCIAL MEDIA

- a. Benefits
 - i. Timely and Cost-Effective Communication
 - 1. Direct Link to Government
 - a. One click access to information
 - b. Eliminates time waiting in line or on hold
 - 2. Cost Savings
 - a. Virtually no cost to public
 - b. Eliminates cost of paper, postage, space for community meetings (streamed online)
 - ii. Creating a Real-Time Public Record
 - 1. Meeting minutes
 - 2. Records
 - 3. Project Proposals
 - 4. Maps
 - 5. Local laws
 - iii. Encourages Social Activism
 - 1. "The New Public Square"
 - 2. Of the e-population, 77% have searched for information from government agencies or communicated with government agencies.
Available at <http://conservancy.umn.edu/handle/51081>
 - 3. Provides a voice to those who cannot or will not attend public meetings.
- b. Government Employee Use of Social Networking Platforms: Horror Stories
 - i. *Police officers post insensitive comments on Facebook*
 - 1. An Albuquerque police officer fatally shot a suspect. The suspect's attorney filed a civil rights suit and subpoenaed the social media pages of all fifty-seven officers who responded to the shooting.

2. The Officer's Facebook page listed his occupation as "human waste disposal." Another officer posted the following comment upon the death of a civil rights attorney who frequently sued the department:
 3. "Tragic I tell ya; just tragic. Hahahaahhahaah good riddance, a special place in hell waiting for her."
 - ii. *DHS Officer Posts Anti-Muslim Comments*
 1. A Department of Homeland Security/TSA Officer was fired after posting hundreds of racist and anti-Muslim comments.
 - iii. *Mayor Tweets Confidential Information*
 1. The mayor of a small Michigan town attempted to maintain transparency in his administration by Tweeting a link to a check register detailing town expenses.
 2. He accidentally Tweeted a link to a report that had personal information and Social Security numbers for 65 town employees. The Tweet went out to 760 Twitter followers.
 3. The town was forced to provide free subscriptions to an identity theft protection service for the employees.
 - iv. *Inappropriate Emails at Work*
 1. A 27-year-old professional woman tells the story of how one of her superiors, a flirty married man with children, who, after overhearing a previous comment she'd made to a female co-worker about buying a new dress, sent her a late- night e-mail from his personal account, telling her he couldn't wait to see her in the dress.
 2. "I'm sure you will look amazing in it," he wrote. The woman responded that she didn't appreciate him sending an e-mail like that to her work account, and he claimed it was a mistake and "half-apologized." Later, he sent her an IM that she feels was "completely inappropriate." She remembers telling her co-workers she would have to block him.
3. LEGAL CONSIDERATIONS
- a. Although social media offers many advantages, it is still an open question as to whether social media can sufficiently replace traditional public forums.
 - i. Serious lack of accountability
 - b. Concerns with the First Amendment; there is a potential minefield of concerns here.
 - i. Area of Law is Very Undeveloped
 1. Proceed with caution or you'll find yourself defending a First Amendment challenge.
 2. There is little guidance from the courts
 - ii. Legal Analysis
 1. Classic Forum Analysis
 - a. Different protections depending upon the forum: The classification of public property is central to determining the scope and extent of free speech. Under traditional First

Amendment forum analysis, there are three types of public property: (1) the traditional “open” public forum; (2) the “closed” or non-public forum; (3) the “designated” public forum; and (4) the “limited” public forum (a sub-category of the designated public forum). *Bowman v. White*, 444 F.3d 967, 974 (8th Cir. 2006).

- i. OPEN – places that are traditionally used for “expressive activities” Public forum property traditionally includes public streets, sidewalks, parks and city squares. See *Hague v. CIO*, 307 U.S. 496, 515, 59 S.Ct. 954, 963, 83 L.Ed. 1423 (1939).

- 1. Strict Scrutiny: restrictions must be narrowly tailored to serve significant government interest

- ii. DESIGNATED – The designated public forum is created when the government intentionally dedicates a non-public forum for expressive conduct by a class of speakers. See *Flint v. Dennison*, 488 F.3d 816, 830 (9th Cir. 2007).

- 1. LIMITED – A limited public forum is “a sub-category of a designated public forum that refer[s] to a type of nonpublic forum that the government has intentionally opened to certain groups or to certain topics.” *Flint v. Dennison*, 488 F.3d at 831 citing *Hopper v. City of Pasco*, 241 F.3d 1067, 1074 (9th Cir.2001).

- a. Here, the government may make distinctions in access and speech on the basis of: (i) subject matter; and (ii) speaker identity. See *Perry Educ. Ass’n v. Perry Local Educators’ Ass’n*, 460 U.S. 37, 49 3d Cir. 2008) i.e. government agency meetings.

- b. Content neutral restrictions can be enforced as long as they are narrowly tailored to serve a significant government interest and leave open alternative channels of communication. *Id.* at 45.

- iii. NONPUBLIC - Includes government property that is not by tradition or designation open for public communication, but used for business, education or other dedicated purposes. The state may reserve non-

public property for its intended purpose, provided that the regulation of speech is reasonable and not an effort to suppress a particular viewpoint. Examples of non-public forums include courthouses, jails, government offices, city halls and public schools. While such state property is required to be open for its devoted purposes, it is not required to be open to the public for other expressive activities. See *Perry Education Assn. v. Perry Local Educators' Assn.*, 460 U.S. 37, 45-46, 103 S.Ct. 948 (1983).

1. Medium Scrutiny

2. Government Speech Doctrine

- a. Government is exempt from First Amendment scrutiny as long as the agency is “engaging in [its] own expressive conduct.” *Pleasant Grove City, Utah v. Summum*, 555 U.S. 460, 467 (2009)(citations omitted).
- i. Not unchecked; government still must comply with establishment clause and voters.

iii. Which Analysis Applies: forum analysis or government speech doctrine?

- 1. OPEN QUESTION; both analyses can apply depending upon the forum created by the government entity. Devala A. Janardan, *Teaching an Old Dog New Tricks*, IMLA J. Loc. Gov’t L., May/June 2010, at 29.
- 2. If a forum is created by the government, then the forum analysis likely applies. HOWEVER, if a nongovernmental forum is created, the government speech doctrine probably applies.

iv. TYPE OF FORUM? OPEN QUESTION

- 1. SETTLED: Social media is NOT a traditional public forum. *United States v. Am. Library Ass’n, Inc.*, 539 U.S. 194, 206 (2003).
- 2. If created, probably designated or limited public forums
 - a. Interactive features more comparable to a public meeting than to a website.
 - b. If users can post comments, links, or any form of communication, the government agency has likely created some type of forum
 - c. If the public agency has completely restricted comments, there is likely no forum. *Hogan v. Township of Haddon*, 278 F. App’x 98, 101-02 (3d Cir. 2008).
- 3. FACEBOOK?
 - a. Where public user can only post comments after “friending” or “liking” the government page, a limited public forum has probably been created.

- b. Government can restrict comments as long as the restrictions are reasonable and viewpoint neutral.
 - c. Open Meeting Laws
 - i. Open meeting laws, also known as “sunshine laws” apply to public decision making bodies.
 - ii. Very little case law applying social media to these laws
 - iii. Case law suggests that courts will focus on the level and nature of the interaction between board members when deciding whether there was a violation of an open meeting law. *See Johnston v. Metropolitan Government of Nashville & Davidson County*, 320 S.W.3d 299; *Wood v. Battle Ground School District*, 27 P.3d 1208.
 - d. The Americans with Disabilities Act
 - i. Be aware that some people are unable to access the internet
 - ii. BE CERTAIN not to use social media and the internet in a way that hampers access of information by certain groups of people
 - 1. Under section 504, any program that receives federal funds cannot exclude any individual with a disability from participating or enjoying the benefits from that program and must provide participants with meaningful access.
 - 2. Information should not be solely available on Facebook or the County website.
 - 3. How is someone who is blind supposed to get this information?
 - 4. GOOD SOURCE David Poteet, Making the Web Usable for the Visually Impaired: Beyond Section 508 Compliance, NewCity (Apr. 17, 2003), <http://www.insidenewcity.com/blog/view/making-the-web-usable-for-the-visually-impaired-beyond-section-508-compliance/> (last accessed Sep. 23, 2013.)
- 4. PUBLIC EMPLOYEE USE OF SOCIAL MEDIA
 - a. Concerns
 - i. Government concern with free speech and social media are not just limited to the public—employees are a large source of concern;
 - ii. It is well settled law that government employees have limited expectations of privacy at work (office, locker, telephone calls)
 - b. Constitutional Protections
 - i. Government employers can dictate what its employees do on social media—to an extent.
 - 1. A government employee does not give away all her free speech rights simply by virtue of her employment. *Pickering v. Bd. of Educ.*, 391 U.S. 563, 568 (1968).
 - ii. When can government restrict speech of public employees?
 - 1. Two Step Analysis
 - a. Matter of Public Concern? If no, then there is no protection.

- i. “typically matters concerning government policies that are of interest to the public at large, a subject on which public employees are uniquely qualified to comment.” *City of San Diego, Cal v. Roe*, 543 U.S. 77, 80 (2004).
- ii. Courts look to the “content, form, and **context** of a given statement, as revealed by the whole record.” *Connick v. Myers*, 461 U.S. 138, 147-48 (1983). (emphasis added)
- iii. Personal gripes about work conditions? Not a matter of public concern and protected to the same degree as that of private employees. *See id.*; *see also Wainwright v. Henry*, 315 F.3d 844, 849 (7th Cir. 2003); *Arvinder v. Mayor & City Council of Balto.*, 862 F.2d 75, 78 (4th Cir. 1988).

b. THE PICKERING BALANCE

- i. If employee is speaking on a matter of public concern, can restrict as long as it is necessary for the government operation
 - 1. “the interests of the [employee] as a citizen, in commenting upon matters of public concern”
AGAINST
 - 2. “the interests of the State, as an employer, in promoting efficiency of public services through its employees”

5. MONITORING EMPLOYEES’ ELECTRONIC COMMUNICATIONS

- a. Under federal law, employers have the right to monitor work-related use of telephone, e-mail, and other computer-generated communications, if certain conditions have been met.
- b. Employees generally do not have a reasonable expectation of privacy in communications sent or received using employer-owned equipment as long as the employer has a policy stating that it can monitor or audit information sent over its systems. *See, e.g., United States v. Angevine*, 281 F.3d 1130 (10th Cir.).
 - i. Does this apply to public employers/employees? Probably not, but safe practice is to have a policy stating that employee’s communications over public systems will be monitored.

C. FEDERAL STORED COMMUNICATIONS ACT

- i. Employers may not access an employee’s private electronic social networking accounts 1) without proper authorization or 2) through illicit or coercive means.
- ii. Employers should not create fictitious online identities in order to troll social networking sites undetected.
- iii. The SCA privacy protections apply only when a provider furnishes ECSs *to the public*. The statute does not define the term “public” but it likely requires that

services be available to any member of the general population who complies with the provider's requisite procedures and pays any requisite fees. An ECS provider does not furnish services to the public, however, if its services are only available to those with a special relationship with the provider, such as when an employer provides e-mail accounts to its employees. *See Andersen Consulting LLP v. UOP*, 991 F.Supp. 1041 (N.D. Ill. 1998). Thus, if a local government establishes and maintains its own internal e-mail system, the SCA does not apply. On the other hand, if a local government contracts with an external provider to furnish e-mail or text messaging services to its employees and officials, the SCA may apply (if other applicable requirements are satisfied).

6. CHECKLIST FOR SOCIAL MEDIA POLICY¹

- a. Should have a STATED PURPOSE; obtaining or conveying information to further goals of the County
- b. ADMINISTRATIVE OVERSIGHT; administrator should be trained to ensure that content furthers the County's goals
- c. COMMENT POLICY;
 - i. Identify the type of content that is not permitted
 - 1. Irrelevant comments
 - 2. Profanity
 - 3. Obscene comments
 - 4. Violent comments
 - 5. Discriminatory comments
 - 6. Solicitation of business
 - 7. Comments that violate copyright or trademark laws
 - 8. Content that violates law
 - ii. Disclaimer, "any comment posted by a member of the public is not an opinion of the County"
 - iii. Policy should state that "Administrator reserves the right to remove content that violates the social networking policy or any applicable law."
- d. EMPLOYEE USAGE POLICY
 - i. Employees should know the County's expectations and restrictions
 - ii. Suggestions
 - 1. Communicate whether social media use in the workplace is allowed, monitored, restricted, etc.
 - a. For example , a social media policy should not ban "inappropriate discussions" about the agency, management, working conditions , or coworkers that would be considered protected speech in another form or forum.

¹ Patricia E. Salkin and Julie A. Tappendorf , Social Media and Local Governments, Navigating the New Public Square 139 (American Bar Association 2013).

2. The policy should also caution employees that they have no expectation of privacy while using the internet on employer equipment. If employees be monitored, then the policy should inform them of such.
3. The policy should also require employees who identify themselves as government staff to post a disclaimer that any postings are solely the opinion of the employee.
4. Employees should be advised not to use the government logo without written consent.
5. The policy should also address the protection of confidential and sensitive government information.
6. Prior to taking any adverse employment action against an employee on account of the content of the employee's comments, consider whether the employee's comments:
 - a. Were posted on a public site accessible to a large number of people
 - b. Disclosed confidential information;
 - c. Were directed at coworkers in a serious effort to discuss working conditions or were simply a venue to vent personal frustration.
7. All employees should be required to sign a written acknowledgment receiving, reading, understanding, and agreeing to comply with the social media policy.